IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

DISH NETWORK, L.L.C., NAGRASTAR LLC,	§	
	§	SA-19-CV-01171-DAE
Plaintiffs,	§	
vs.	§	
ARNOLDO DEL CARMEN,	§	
Defendant.	§	

REPORT AND RECOMMENDATION
OF UNITED STATES MAGISTRATE JUDGE

To the Honorable United States District Judge David A. Ezra:

This Report and Recommendation concerns the Motion for Default Judgment filed by Plaintiffs Dish Network LLC and Nagrastar LLC [#8]. The motion was referred to the undersigned for disposition on January 31, 2020. The undersigned has authority to enter this recommendation pursuant to 28 U.S.C. § 636(b)(1)(B). For the reasons set forth below, it is recommended that Plaintiffs' Motion [#8] be **GRANTED**.

I. Jurisdiction

This court has diversity jurisdiction over this action under 28 U.S.C. § 1331 because this action alleges violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1201, *et seq.*, the Federal Communications Act, 47 U.S.C. § 605, *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511, *et seq.* (Compl. [#1] at ¶ 4.)

II. Procedural History

Plaintiffs DISH Network LLC and Nagrastar LLC ("Plaintiffs") filed this action against Defendant Arnoldo Del Carmen ("Defendant") on September 27, 2019, alleging that Defendant has been trafficking in server passcodes that are designed and used solely for purposes of

circumventing Plaintiffs' security system and receiving DISH Network's (hereinafter "DISH") satellite broadcasts of copyrighted television programming without payment of the required subscription fee. (Compl. [#1] at ¶ 7.) Plaintiffs further contend that Defendant personally used server passcodes to decrypt DISH's satellite signal and view its programming without authorization. (*Id.*) According to Plaintiffs, these acts violate the Digital Millennium Copyright Act, the Federal Communications Act, and the Electronic Communications Privacy Act. (*Id.*) By this action, Plaintiffs seeks a permanent injunction restraining and enjoining Defendant and all persons acting on his behalf from trafficking in server passcodes and intercepting satellite transmissions without authorization, as well as other related injunctive relief, and actual and punitive damages, costs, and fees. (*Id.* at 10–13.)

The record reflects that Defendant was served with Plaintiffs' Summons and Complaint on October 5, 2019, making his answer due on October 28, 2019 [#5]. To date, Defendant has failed to file an answer or otherwise make an appearance in this case. Plaintiffs moved for a Clerk's Entry of Default, which was granted and entered on December 16, 2019 [#7]. Plaintiffs now move for a Final Default Judgment against Defendant on Counts I and II of their Complaint, which allege violations of the Digital Millennium Act ("DMCA") and the Federal Communications Act ("FCA").

In order to ensure that Defendant received a copy of Plaintiffs' Motion for Default Judgment, as well as an opportunity to cure his default, the Court ordered the District Clerk's Office to mail a copy of the motion to Defendant at his address on record, and further ordered Defendant to respond to the motion on or before February 25, 2020 [#9]. The District Clerk's Office mailed a copy of the pertinent court filings via first-class mail and certified mail, return receipt requested, to Defendant's addresses on file [#10]. The Court received confirmation of

delivery on February 10, 2020 [#11]. Defendant has not filed a response to Plaintiffs' motion or made an appearance in this action, and all of the Court's deadlines to do so have expired.

III. Legal Standard

"When a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise, the clerk must enter the party's default." Fed. R. Civ. P. 55(a). Once default has been entered, the court may enter a default judgment against the defaulting defendant upon motion by the plaintiff. *See* Fed. R. Civ. P. 55(b); *N.Y. Life Ins. Co. v. Brown*, 84 F.3d 137, 141 (5th Cir. 1996). In considering a motion for default judgment, the court accepts as true the well-pleaded allegations of facts in the complaint (except regarding damages) but must determine whether those facts state a claim upon which relief may be granted. *See Matter of Dierschke*, 975 F.2d 181, 185 (5th Cir. 1992) (stating that a defaulting party is deemed to have admitted all well-pleaded allegations of the complaint); *United States ex rel. M-Co. Constr., Inc. v. Shipco Gen., Inc.*, 814 F.2d 1011, 1014 (5th Cir. 1987). Thus, for a plaintiff to obtain a default judgment, "[t]here must be a sufficient basis in the pleadings for the judgment entered." *Nishimatsu Constr. Co., Ltd. v. Houston Nat'l Bank*, 515 F.2d 1200, 1206 (5th Cir. 1975); *see Lewis v. Lynn*, 236 F.3d 766, 767 (5th Cir. 2001) ("[A] party is not entitled to a default judgment as a matter of right, even where the defendant is technically in default.") (quoting *Ganther v. Ingle*, 75 F.3d 207, 212 (5th Cir. 1996)).

IV. Analysis

The record in this case establishes that Defendant failed to plead or otherwise defend against Plaintiffs' claims. Defendant was served with a copy of Plaintiffs' Complaint but failed to answer or otherwise respond. The undersigned therefore finds that the Clerk properly entered default, and Plaintiffs are entitled to default judgment on Counts I and II of their Complaint

because the facts alleged in Plaintiffs' Complaint as to these two claims state a claim upon which relief can be granted.

A. Allegations in Plaintiffs' Complaint

Plaintiffs' Complaint alleges the following: DISH uses high-powered satellites to broadcast television programming to millions of subscribers in the United States who pay DISH a subscription fee to receive such programming, or in the case of a pay-per-view program, the purchase price. (Compl. [#1] at ¶ 8.) NagraStar provides smart cards and other proprietary security technologies that form a conditional access system. (*Id.*) DISH contracts for and purchases the right to broadcast the television programming shown on its platform from networks, motion picture distributors, pay and specialty broadcasters, sports leagues, and other rights holders. (*Id.* at ¶ 9.) The works broadcast by DISH are copyrighted, and DISH and NagraStar have the authority of the copyright holders to protect the works from unauthorized reception and viewing. (*Id.* at ¶ 10.)

DISH programming is digitized, compressed, and scrambled prior to being transmitted to multiple satellites located in geo-synchronous orbit above Earth. (*Id.* at ¶ 11.) The satellites, which have relatively fixed footprints covering the United States and parts of Canada, Mexico, and the Caribbean, relay the encrypted signal back to Earth where it can be received by DISH subscribers that have the necessary equipment. (*Id.*) A DISH satellite television system consists of a compatible dish antenna, receiver, smart card (which in some instances is internalized in the receiver), television, and cabling to connect the components. (*Id.* at ¶ 12.) DISH provides receivers, dish antenna, and other digital equipment for the DISH system; NagraStar supplies the smart cards and other proprietary security technologies that form a conditional access system. (*Id.*) Each DISH receiver and NagraStar smart card is assigned a unique serial number that is

used by DISH when activating the equipment and to ensure the equipment only decrypts programming the customer is authorized to receive as part of his subscription package and pay-per-view purchases. (*Id.* at ¶ 13.) Together, the DISH receiver and NagraStar smart card convert DISH's encrypted satellite signal into viewable programming that can be displayed on the attached television of an authorized DISH subscriber. (*Id.* at ¶ 16.)

A form of satellite piracy—i.e. the unauthorized reception, decryption, or viewing of a pay-tv signal—exists that goes by several names, including "control word sharing," "Internet key sharing," or more simply "IKS." (*Id.* at ¶ 17.) With IKS, once piracy software is loaded onto an unauthorized receiver, the end user connects the receiver to the Internet via a built-in Ethernet port or an add-on dongle. (*Id.* at ¶ 18.) The Internet connection automatically updates piracy software on the receiver and contacts a computer server that provides the necessary control words. (*Id.*) The computer server, called an "IKS server," has multiple, subscribed NagraStar smart cards connected to it, and thus the ability to provide the control words. (*Id.* at ¶ 19.) Access to an IKS server typically requires a valid passcode. (*Id.*) Once access has been obtained, control words are sent from the IKS server over the Internet to an unauthorized receiver, where they are used to decrypt DISH's signal and view programming without paying a subscription fee. (*Id.*)

IKSRocket is a subscription-based IKS service, whereby members purchase a subscription to the IKS service to obtain the control words that are used to circumvent the DISH and NagraStar security system and receive DISH's satellite broadcasts of television programming without authorization. (*Id.* at ¶ 20.) Digital TV is a Dominican Republic company that sold subscriptions to IKSRocket ("IKS Server Passcodes"). (*Id.* at ¶ 21.) Digital TV provided DISH and NagraStar with copies of its business records pertaining to Defendant. (*Id.*)

Digital TV's records show that Defendant purchased at least 46 IKS Server Passcodes within the statute of limitations for each claim that Plaintiffs are bringing against Defendant. (*Id.*) Each IKS Server Passcode that Defendant purchased is believed to have been valid for one year. (*Id.*)

Plaintiffs plead on information and belief that Defendant re-sold certain IKS Server Passcodes that he purchased from Digital TV. (*Id.* at ¶ 22.) These IKS Server Passcodes enabled Defendant's customers to access the IKSRocket service using an unauthorized receiver loaded with piracy software. (*Id.*) Each time that the customer tuned their unauthorized receiver to an encrypted DISH channel, the receiver requested the control word for that particular channel from the IKS server. (*Id.*) The IKS servers then returned the NagraStar control word, which the customer used to decrypt DISH's satellite signal and view DISH programming without purchasing a subscription from DISH. (*Id.*) Plaintiffs also plead on information and belief that Defendant also used certain IKS Server Passcodes that he purchased for his own personal benefit. (*Id.* at ¶ 23.) Defendant is believed to have used an IKS Server Passcode in connection with an unauthorized received loaded with piracy software to access the IKS service. (*Id.*)

Plaintiffs contend that Defendant's actions have caused actual and imminent irreparable harm for which there is no adequate remedy at law. (*Id.* at ¶ 24.) Through IKS piracy, Defendant has unlimited access to DISH programming, including premium and pay-per-view channels, causing lost revenues that cannot be fully calculated. (*Id.*) In addition, Defendant's actions damage the business reputations and goodwill of Plaintiffs and result in the need for costly and continuous security updates, investigations, and legal actions aimed at stopping satellite piracy. (*Id.*)

B. Plaintiffs have adequately pleaded that Defendant violated the Digital Millennium Copyright Act and the Federal Communications Act.

Plaintiffs request default judgment on Counts I and II of their Complaint, which allege violations of the DMCA and the FCA. The DMCA prohibits trafficking in any technology, service, or part thereof that: (1) is designed or produced for circumventing a measure that effectively controls access to a copyrighted work; (2) has only limited commercial purpose or use other than circumventing an access control measure; or (3) is marketed for use in circumventing an access control measure. 17 U.S.C. § 1201(a)(2). To circumvent an access control measure "means to descramble a scrambled work, to decrypt an encrypted work, or to otherwise avoid, bypass, remove, deactivate, or impair a technological measure." *Id.* § 1201(a)(3)(A).

Plaintiffs' encryption-based security system constitutes an effective access control measure for purposes of the DMCA. *See DISH Network L.L.C. v. Sonicview USA, Inc.*, No. 09-cv-1533-L

(WVG), 2012 WL 1965279, at *8 (S.D. Cal. May 31, 2012) (holding that encryption-based systems are control measures under DMCA); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (holding that security measures based on "encryption or scrambling" are effective for purposes of the DMCA).

Section 605(e)(4) of the FCA is similar and makes it unlawful for any person to import or distribute any device or equipment "knowing or having reason to know" it "is primarily of assistance in the unauthorized decryption of . . . direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a)." 47 U.S.C. § 605(e)(4). Subsection (a) provides that "[n]o person not being entitled thereto shall receive or assist in receiving any

interstate or foreign communication by radio and use such communication . . . for his own benefit or for the benefit of another not entitled thereto." *Id.* § 605(a). DISH's satellite television broadcasts are direct-to-home satellite services for purposes of section 605(e)(4), and protected radio communications under section 605(a). *See Sonicview USA*, 2012 WL 1965279, at *10; *Garden City Boxing Club Inc. v. Cardenas*, No. CIV.A. H-05-3318, 2006 WL 2713817, at *2 (S.D. Tex. Sept. 21, 2006). The DMCA and FCA apply to various piracy instruments including passcodes. *See* 17 U.S.C. § 1201(a)(2) (encompassing "any technology, product, service, device, component, or part thereof"); *DISH Network LLC v. DiMarco*, No. 2:11-cv-01962, 2012 WL 917812, at *5 (D. Nev. March 14, 2012) (finding DMCA applicable to the distribution of passwords used to access IKS servers); *Dish Network LLC v. Dillion*, No. 12CV157 BTM NLS, 2012 WL 368214, at *3–4 (S.D. Cal. Feb. 3, 2012) (finding DMCA and FCA apply to piracy-enabling software files).

Plaintiffs have adequately pleaded that Defendant trafficked in IKS Server Passcodes in violation of section 1201(a)(2) of the DMCA and section 605(e)(4) of the FCA. Moreover, Plaintiffs provide the Court with the Declaration of Christopher Ross, an intelligence analyst for NagraStar, primarily responsible for investigating piracy matters affecting NagraStar security technology, including that used by DISH to protect its satellite broadcasts of television programming. (Ross Decl. [#8-3] at ¶ 1.) Ross attests that he participated in the investigation of IKSRocket, reviewed the records of the confidential information that managed the sale of IKSRocket through Digital TV, and identified Defendant as a purchaser of IKS Server Passcodes. (*Id.* at ¶¶ 3–5.) Attached to Ross's declaration is a copy of the file obtained from these records containing identifying information connecting Defendant to these purchases. (*Id.* at ¶¶ 6–8; Exhibits to Ross Decl. [#8-4, #8-5, #8-6].) This evidence demonstrates that Defendant

purchased enough IKS Server Passcodes that, if retained for personal use, would last him 46 years.

C. Plaintiffs should be awarded statutory damages under the DMCA.

Plaintiffs' motion establishes that they are entitled to recover statutory damages under the DMCA. Rule 55(b) provides a court with discretion to convene an evidentiary hearing on the issue of damages. Fed. R. Civ. P. 55(b)(2). When a party seeks default judgment, damages ordinarily may not be awarded "without a hearing or a demonstration by detailed affidavits establishing the necessary facts." *United Artists Corp. v. Freeman*, 605 F.2d 854, 857 (5th Cir. 1979). However, where the amount of damages can be "determined with certainty by reference to the pleadings and supporting documents," and where a hearing would reveal no pertinent information, "the court need not jump through the hoop of an evidentiary hearing." *James v. Frame*, 6 F.3d 307, 310-11 (5th Cir. 1993) (a district court has "wide latitude" in deciding whether to require an evidentiary hearing when granting default judgment). Here, Plaintiffs do not request a hearing, have moved only for statutory as opposed to actual damages, and has attached detailed affidavits to their motion from which the Court may calculate damages. Accordingly, an evidentiary hearing to determine damages is unnecessary.

1. Statutory damages under the DMCA in the amount of $2,500 per violation are sufficient and reasonable.

Under the FCA, an aggrieved party may be awarded statutory damages for each violation of Section 605 "in a sum of not less than $1,000 or more than $10,000, as the court considers just." 47 U.S.C. § 605(e)(3)(C)(i)(II). Under the DMCA, an aggrieved party may be awarded statutory damages for each violation of Section 1201 "in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just." 17 U.S.C. § 1203(c)(3)(A). Plaintiffs request the statutory

maximum for each of Defendant's violations—$10,00 per infringing product under the FCA. Because the record establishes that Defendant purchased 46 IKS Server Passcodes, Plaintiffs ask the Court to award $460,000 in statutory damages. Alternatively, if damages are not awarded under the FCA, Plaintiffs request the statutory maximum of $2,500 per IKS Server Passcode under the DMCA for a total of $115,000 in compensatory damagse. Plaintiffs are not seeking an award of attorneys' fees or costs in their final default judgment. For the reasons that follow, the Court should award Plaintiffs the maximum statutory damages under the DMCA and not the FCA.

In support of its request for $10,000 in statutory damages under the FCA, Plaintiff proffers the declaration of Gregory Duval, Chief Operating Officer with NagraStar. (Duval Decl. [#8-2] at ¶ 2.) According to Duval, Plaintiffs' businesses are damaged extensively by the piracy at issue in this case. DISH and NagraStar invest millions of dollars each year in security measures that protect DISH programming. (Duval Decl. [#8-2] at ¶ 17.) The distribution of products that circumvent these security measures undermines Plaintiffs' investment in these technologies and results in the need for costly security updates and anti-piracy countermeasures. (*Id.* at ¶ 17–18.) Piracy also interferes with contractual and prospective business relationships of Plaintiffs; causes damage to the goodwill and reputations of Plaintiffs; and results in lost sales and programming revenues. (*Id.* at ¶ 19–20.)

Plaintiffs direct the Court to several cases in which plaintiffs have been awarded the maximum available statutory damages under the FCA in analogous circumstances. (*See* Pls.' Mem. [#8-1] at 6 (collecting cases).) Yet other cases have refused to award the maximum damages available under the FCA in analogous situations, reasoning that the actual loss to the plaintiffs (the amount that would have been received from legitimate subscriptions) was much

lower. *See, e.g.*, *DISH Network L.L.C. v. Simmons*, No. 4:17-CV-53, 2018 WL 3647169, at *6 (E.D. Tenn. June 28, 2018), *report and recommendation adopted*, No. 4:17-CV-53, 2018 WL 3623764 (E.D. Tenn. July 30, 2018) (rejecting request for $560,000 in statutory damages (for 56 IKS Server Passcodes) based on an estimate of only $84 per month in lost programming revenues per IKS Server Passcode)). An identical statement is contained in the declaration before the Court in this case (made by the same declarant in the *Simmons* case), estimating lost programming revenues in the average amount of $84 per month per subscriber. (Duval Decl. [#8-2] at ¶ 20.) In *Simmons*, the court reasoned that actual damages were approximately $56,448 ($84 for each of the 56 IKS Server Passcodes pirated times 12 months, as each passcode was valid for one year). *Simmons*, 2018 WL 3647169, at *6. The court could not "reconcile a penalty of statutory damages that is ten time the estimated loss" and therefore instead chose to award statutory damages under the DMCA at the lower rate of $2,500 for each violation. *Id.* at *6–7.

The Court agrees with the *Simmons* court that there is a significant discrepancy between the $460,000 in statutory damages requested here and the estimated loss of $46,368 in lost subscriptions from Defendant ($84 for each of the 46 IKS Server Passcodes pirated by Defendant times 12 months). However, the Court also recognizes that $46,368 does not account for the fact that Defendant re-sold the IKS Server Passcodes he purchased to an unidentifiable number of other potential subscribers, compounding lost programming revenues. (Compl. [#1] at ¶ 22.) Accordingly, the actual lost programming revenues here was likely much higher than $46,368, although still likely well under $460,000. In light of the foregoing, the Court is persuaded that an award of $460,000 is excessive and will instead look to the maximum statutory damages available under the DMCA to remedy Defendant's violations.

Again, Plaintiffs request the statutory maximum of $2,500 per IKS Server Passcode or $115,000 under the DMCA as an alternative to FCA statutory damages. Courts have broad discretion in determining the amount of statutory damages to award under the DMCA between the prescribed range of $200 to $2,500. *See* 17 U.S.C. § 1203(c)(3)(A) (authorizing an award of statutory damages "for each violation of section 1201 in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just"); *Peer Int'l Corp. v. Pausa Records, Inc.*, 909 F.2d 1332, 1336 (9th Cir. 1990) (recognizing wide discretion of courts in determining appropriate level of statutory damages); *Cable/Home Commc'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 852 (11th Cir. 1990) (same). When determining the amount of damages for each violation, courts consider the willfulness of the conduct as well as the need for deterrence. *See Sony Computer Entm't Am., Inc. v. Filipiak*, 406 F. Supp. 2d 1068, 1074–75 (N.D. Cal. 2005); *Tracfone Wireless, Inc. v. SND Cellular, Inc.*, 715 F. Supp. 2d 1246, 1261–62 (S.D. Fla. 2010). Within the context of the DMCA, "willful" means acting with knowledge that the product is designed or used for circumvention. *See Filipiak*, 406 F. Supp. 2d at 1075 (applying the definition of willfulness used in copyright infringement context in construing the DMCA).

The pleadings and evidence before the Court establish that Defendant's conduct was indeed willful, as he purchased 46 IKS Server Passcodes, used solely to access the IKSRocket service and obtain control words to illegally decrypt DISH's satellite signal. Moreover, according to Plaintiffs' allegations, deemed admitted here, Defendant re-sold these passcodes to other individuals. The amount imposed as damages should serve to deter Defendant from engaging in future similar conduct. Accordingly, Plaintiffs should be awarded $115,000 in statutory compensatory damages.

2. Plaintiffs should be awarded a permanent injunction.

In addition to statutory damages, Plaintiffs request a permanent injunction pursuant to the Federal Rules of Civil Procedure and the DMCA. *See* Fed. R. Civ. P. 65; 17 U.S.C. § 1203(b)(1) ("[T]he court . . . may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation."). For permanent injunction to issue, Plaintiffs must demonstrate the following: (1) that they have suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that considering the balance of hardships between the parties, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction. *eBay, Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006). The requirements for permanent injunctive relief are satisfied in this case.

First, Plaintiffs have suffered an irreparable injury in their loss of goodwill, their ability to control their business reputation, and their lost profits. *See Emerald City Mgmt., L.L.C. v. Kahn*, 624 Fed. App'x 223, 224 (5th Cir. 2015) (finding that loss of control over reputation and goodwill cannot be quantified and thus constitutes irreparable harm). Plaintiffs' Complaint and the evidence before the Court establishes that Plaintiffs invest millions of dollars each year in security measures to protect DISH programming from unauthorized viewing. (Duval Decl. [#8-2] at ¶ 17.) The type of piracy employed by Defendant is designed to circumvent a security technology most recently introduced by Plaintiffs, which took approximately 18 months to implement and had an estimated cost of more than $100 million. (*Id.* at ¶ 18.) As a result of piracy like that of Defendants, Plaintiffs are forced to continually develop anti-piracy countermeasures, at significant expense. (*Id.*)

Secondly, Plaintiffs' damages are difficult if not impossible to quantify, making monetary damages inadequate to compensate them fully for their injuries. As previously noted, it is challenging to quantify and measure the scope of damage to Plaintiffs' businesses caused by Defendant's actions and related piracy, as those involved in piracy (like Defendant) often re-sell the IKS Server Passcodes to others, making it impossible to determine the exact number of persons involved and the scope of Plaintiffs' losses. (*Id*.) Calculating reputational damage is equally difficult to quantify.

Finally, the balance of hardships between the parties and the public interest favor permanent injunctive relief. The only harm to Defendant resulting from an injunction would be his loss of revenue from the sale of infringing products, which should not be given weight. *See Dish Network LLC v. Barnaby*, No. 3:15-CV-492-TAV-HBG, 2016 WL 6603202, at *6 (E.D. Tenn. Nov. 8, 2016) (citing *Cadence Design Sys., Inc. v. Avant! Corp.*, 125 F.3d 824, 829 (9th Cir. 1997) (finding that profits lost from the enjoined sales of infringing goods is not cognizable harm); *Triad Sys. Corp. v. Se. Express Co.*, 64 F.3d 1330, 1338 (9th Cir. 1995) ("[The defendant] cannot complain of the harm that will befall it when properly forced to desist from its infringing activities.")). The public interest is served by enjoining violations of federal law. *See Motown Record Co. v. Armendariz*, No. SA-05-CA-0357 XR, 2005 WL 2645005, at *4 (W.D. Tex. Sept. 22, 2005) (finding it to be in the public interest to enjoin defendant's infringing conduct in order to uphold copyright protections).

The Court further finds that the proposed permanent injunction is narrowly tailored to restrain Defendant from violating Plaintiffs' rights. Defendant has been trafficking in IKS Server Passcodes, thereby enabling end users to circumvent Plaintiffs' security system and

receive DISH programming without authorization. The Court should enjoin Defendant, and anyone acting in concert with Defendant, from the following:

- manufacturing, importing, offering to the public, providing, or otherwise trafficking in IKS Server Passcodes, any other code or password used in accessing an IKS Server, and any other technology or part thereof that is used in circumventing Plaintiffs' security system or receiving DISH programming without authorization;
- circumventing or assisting others in circumventing Plaintiffs' security system, or receiving or assisting others in receiving DISH's satellite signal without authorization; and
- testing, analyzing, reverse engineering, manipulating, or extracting code, data, or information from Plaintiffs' satellite receivers, smart cards, satellite stream, or any other part or component of Plaintiffs' security system.

V. Conclusion and Recommendation

Having considered Plaintiffs' motion, Complaint, and evidence, the entire case file, and the lack of response from Defendant, the undersigned recommends that the Motion for Default Judgment filed by Plaintiffs Dish Network LLC and Nagrastar LLC [#8] be **GRANTED** and the proposed default judgment be entered against Defendant [#8-7], with the exception that statutory damages be awarded in the amount of $115,000 in accordance with 17 U.S.C. § 1203(c)(3)(A) as opposed to the proposed maximum damages under the FCA.

VI. Instructions for Service and Notice of Right to Object/Appeal.

The United States District Clerk shall serve a copy of this report and recommendation on all parties by either (1) electronic transmittal to all parties represented by attorneys registered as

a "filing user" with the clerk of court, or (2) by mailing a copy to those not registered by certified mail, return receipt requested. Written objections to this report and recommendation must be filed **within fourteen (14) days** after being served with a copy of same, unless this time period is modified by the district court. 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b). The party shall file the objections with the Clerk of Court and serve the objections on all other parties. A party filing objections must specifically identify those findings, conclusions or recommendations to which objections are being made and the basis for such objections; the district court need not consider frivolous, conclusive or general objections. A party's failure to file written objections to the proposed findings, conclusions and recommendations contained in this report shall bar the party from a *de novo* determination by the district court. *Thomas v. Arn*, 474 U.S. 140, 149–52 (1985); *Acuña v. Brown & Root, Inc.*, 200 F.3d 335, 340 (5th Cir. 2000). Additionally, failure to file timely written objections to the proposed findings, conclusions and recommendations contained in this report and recommendation shall bar the aggrieved party, except upon grounds of plain error, from attacking on appeal the un-objected-to proposed factual findings and legal conclusions accepted by the district court. *Douglass v. United Servs. Auto. Ass'n*, 79 F.3d 1415, 1428–29 (5th Cir. 1996) (en banc).

SIGNED this 13th day of March, 2020.

ELIZABETH S. ("BETSY") CHESTNEY
UNITED STATES MAGISTRATE JUDGE